AMENDMENT TO THE CLAIMS

Claims 1-36 and 45-50 were canceled with a preliminary amendment.

Claims 1-36 canceled

37.(currently amended) A transmission system for transmitting information from an originator to a mobile device, the transmission system comprising:

an originator component configured to receive the information to be transmitted and form a transmission message; and

~~a receiver component configured to receive the transmission message;~~

wherein the originator includes:

a first encryption key component configured to derive a first encryption key based on a base key known by the receiver component, a first data string and a data portion including transmission message specific data derived from the information to be transmitted;

a second encryption key component configured to derive a second encryption key based on the base key, a second data string and the data portion;

an encryptor configured to hash the information to be transmitted with the first encryption key to obtain a signature and to encrypt the information and the signature with the second encryption key to obtain an encrypted message; and

a joiner configured to join the encrypted message with the transmission message specific data, in unencrypted form.

38.(original) The transmission system of claim 37 wherein the originator comprises:

    a header generation component configured to receive the encrypted message and message specific data and add a header thereto to obtain the transmission message.

39.(currently amended) The transmission system of claim 37 wherein the first encryption key component hashes the base key, the first data string and the_transmission message specific data to obtain a bias value and wherein the first encryption key component includes:

    a key generator configured to receive the bias value and generate the first encryption key based on the bias value.

40. (currently amended) The transmission system of claim 37 wherein the second encryption key component hashes the base key, the second data string and the transmission message specific data to obtain a bias value and wherein the second encryption key component includes:

    a key generator configured to receive the bias value and generate the second encryption key based on the bias value.

41.(original) The transmission system of claim 37 wherein the originator includes:

    a checksum component configured to calculate a checksum over the transmission message and append the checksum thereto.

42.(currently amended) The transmission system of claim 41 ~~wherein the~~and further comprising a receiver component ~~comprises~~comprising:

a processor component; and

a driver component coupled to the processor component;

wherein the ~~processing~~ processor component is configured to receive the transmission message and pass the transmission message to the driver component, the driver component being configured to derive the first and second encryption keys from the ~~based~~ base key, the first and second data strings and the <u>transmission</u> message specific data and decrypt the transmission message.

43. (original) The transmission system of claim 42 wherein the driver component further comprises:

a validation component configured to calculate a checksum over the unencrypted transmission message, and compare the checksum calculated to the checksum calculated by the checksum component to determine whether the unencrypted message is valid.

44. (original) The transmission system of claim 37 wherein the mobile device includes a radio receiver having values stored therein, the values determining operation of the radio receiver, and wherein the transmission message comprises a programming message for programming the values in the radio receiver.

Claims 45 - 50 Canceled